SECURITY AT LAWRENCE LIVERMORE NATIONAL LABORATORY

Hearing of the U.S. House of Representatives Committee on Commerce
Subcommittee on Oversight and Investigations
July 20, 1999

C. Bruce Tarter, Director
Lawrence Livermore National Laboratory
University of California

OPENING REMARKS

Mr. Chairman and members of the committee, I am the Director of the Lawrence Livermore National Laboratory (LLNL). Our Laboratory was founded in 1952 as a nuclear weapons laboratory, and national security continues to be our central mission. Livermore is a principal participant in the Department of Energy's Stockpile Stewardship Program, heavily involved in programs to prevent the proliferation of weapons of mass destruction, and engaged in energy, environmental, and bioscience R&D as well as industrial applications of our core technologies.

Our National Security mission and safeguards and security are inextricably linked, and we take both of them very seriously at Livermore. We cannot carry out our National Security mission effectively without appropriate protection of classified and sensitive information and materials. Like National Security, safeguards and security continues to evolve in terms of requirements and objectives. We have an extensive security and counterintelligence infrastructure in place at our Laboratory, and we continually make adjustments and upgrades to address new threats and concerns. Through a process of internal self-assessments, technical consultants, and external reviews, we ensure our readiness to deal with a broad spectrum of threats. At Livermore, we believe our Special Nuclear Materials (SNM) and sensitive and classified information are secure.

The review recently conducted by the Office of Security Evaluations (OSE) was helpful in identifying areas for improvement. The OSE concluded that in two key areas, Physical Security which deals with the technical systems that help protect Special Nuclear Material, and Classified Cyber Security, which deals with the protection of our classified computing networks, the Laboratory received the highest possible rating.

That is not to say we do not have work to do. Opportunities for improvement were noted in all areas of the OSE report, and the Laboratory is firmly committed to addressing them. I would like to assure you that the concerns raised in the OSE report are receiving high priority, and resources are being made available by the Laboratory to address them.

We have invested heavily in enhanced employee training in security at Livermore. In April, we underwent an intensive two-day cyber security stand-down in which we addressed not only cyber security, but also conducted formal sessions on general security requirements and counterintelligence. In June, in response to Secretary Richardson's five-point Security Immersion Program, we ceased all normal operations for two additional days of security training. Our employees were fully engaged in these training programs, and have made many suggestions for further improving security.

One concern raised by the OSE team had to do with the mixed Q and L clearance environment in the Limited Area of the Laboratory. In recent years, DOE's goal has been to reduce the number of Q clearances. This has been accompanied by an increase in the number of individuals having an L clearance. These are individuals who are allowed physical access to the Limited Area but who do not have access to weapons data. For the record, I would like to note that there are no foreign nationals at LLNL with an L clearance. Any LLNL foreign national visiting the Limited Areas has always required an escort. Within the Limited Area, we rely largely on administrative controls to prohibit access to

classified information by L-cleared personnel. We believe that, although well intended, the reduction in Q clearances has lessened security, and we would like to see funding made available for Q-clearances for all personnel requiring access to the Limited Area of the Laboratory.

The Annual Report to the President on Safeguards and Security rated LLNL "Unsatisfactory" in the area of Materials Control and Accountability (MC&A) and "Marginal" overall. More recently, the April/May OSE Inspection rated LLNL "Marginal" in this MC&A area. In a letter to Assistant Secretary Vic Reis dated May 14, 1999, I personally assured him that the Laboratory was committed to rectifying the rating in MC&A before the end of the calendar year. I would like to note that we are on schedule in our action plan, with most actions already complete. Similarly, in that same letter to Dr. Reis, I committed to funding and implementing the LLNL Tri-Lab INFOSEC Action Plan as approved by DOE. Again, many actions have already been completed and we continue to be on schedule. I note these formal commitments in that they also address some of the concerns raised in the OSE evaluation.

The OSE team was careful to note in their report major improvements made in the Safeguards and Security program to address past concerns, and these improvements are continuing. There have been important technical upgrades to the Perimeter Intrusion Detection and Alarm System (PIDAS) that surrounds our Superblock, which contains our Plutonium facility, to provide early detection of both airborne and bridging attacks. We have recruited and put in place an offensively trained Special Response Team having the training necessary to implement a recovery or recapture action. One hundred percent searches are conducted at material access area portals in the Plutonium Facility. Over 100 simulations of adversary attacks have been completed, and we are continuing to refine our simulation methodology, attack scenarios, and defensive strategies. We have engaged an

external advisory group of very senior former military and FBI experts to advise us in this work. Since the completion of the OSE SE we have committed additional officers to the Superblock and taken other compensatory measures to assure the security of our SNM assets.

Other improvements noted in the OSE report include the installation of an intrusion detection system in a building inside the Limited Area used for the storage of classified non-SNM weapons parts. Alarm systems are now in design for two other facilities in the Limited Area. Foreign Ownership, Control or Influence (FOCI) reviews of all contractors have been completed. A baseline inventory of plutonium has been completed, and improved procedures to ensure effective and timely accounting for any inventory differences have been put in place.

In the area of cyber security, we have already implemented many elements of the Tri-Lab Committee's "nine point plan." For example, steps have been taken to ensure the physical incompatibility of removable media between classified and nearby unclassified computer systems. Scanning of outgoing e-mail has been instituted, and funding has been committed for implementation of a multi-level system that will separate sensitive unclassified computer processing from the remainder of unclassified processing. The frequency of vulnerability scans of network computers is being increased, and unclassified archives are being scanned for classified content. To date over 4 million files have been scanned, and no classified content has been found. Procedures for authorizing access to unclassified computers by foreign nationals have been tightened, and today no foreign nationals have access to Livermore unclassified computer networks without having gone through an indices check and having a formal computer security plan approved by the Laboratory. All dial-up access by foreign nationals is routed through a common terminal server which has special intrusion detection software.

In summary, safeguards and security go hand in hand with our National Security mission at Livermore. We are committed to an excellent safeguards and security program, and have been taking, and will continue to take, the steps necessary to achieve it.

PHYSICAL SECURITY AT LIVERMORE

Livermore's security construct is based on a series of defensive layers—a graded approach that provides increasing barriers that correspond to the increasing value of critical Laboratory assets.

Clearances, badging, and background checks on Laboratory employees (including subcontractors) constitute a first line of defense. Those people with access to classified assets undergo background investigations associated with DOE Q, L or sensitive compartmented information (SCI) clearances as appropriate. Reinvestigations are scheduled automatically at five-year intervals or as needed on a for-cause basis.

Livermore uses a defense-in-depth approach to physical barriers—fences, doors, repositories, and vaults. The Laboratory's outer perimeter fence provides the basic physical protection to U.S. government property. Additional protection is provided for "limited" areas where classified assets are present. The level of clearance required to freely transit these areas is also higher. Classified parts and materials are provided additional physical protection and access control. Significant quantities of special nuclear material receive the highest level of protection, with vault-like physical protection as well as aggressive armed defense and response capabilities.

At each physical barrier (e.g., fence, building, vault), there are various levels of access control. Access control is performed either by security officers or automated security

access portals. At more restricted areas, access is checked against specific access lists. Need-to-know is required, in addition to the appropriate clearance, before an individual is allowed access to classified assets.

The Laboratory employs security officers who are fully trained and accredited to meet DOE criteria. The level of training varies with the assignment (defensive, offensive, or special response). We currently have over 40 offensively trained officers in our Special Response Team and have a new group beginning academy training next month. Training is extensive and performance based. The security force undergoes regular performance tests, self-assessments, DOE surveillance, and inspections.

Physical security is designed into new facilities and facility modifications. Detection systems are continuously monitored and routinely tested. The Laboratory's security system is prepared for armed response to all unauthorized intrusions.

In the Annual Report to the President on Safeguards and Security we received a "Marginal" rating overall but, an "Unsatisfactory" rating in MC&A. The issue involved our inability to meet SNM inventory requirements at a time when the Plutonium Facility was shut down to address safety concerns, preventing monitoring and measurements. Now that safety concerns have been addressed and the facility reopened, we have resumed all special nuclear material measurements and inventory monitoring and we believe we will be in compliance with DOE requirements.

We have high confidence in our Safeguards and Security programs and in the security of our critical assets. We have implemented technical and procedural enhancements to strengthen our physical security, remedied material control and accounting deficiencies, and fully upgraded our strategy to protect nuclear material at our Laboratory.

CYBER SECURITY AT LIVERMORE

Cyber or computer security is a critical element of Livermore's overall security construct. The Laboratory has both classified computer networks and unclassified computer networks. The two are separate and are not connected. We also have numerous stand-alone computer systems and local area networks in both classified and unclassified areas. There are no connections from Livermore's classified computers to the outside world except through NSA-approved encryption.

In addition to physical barriers between the unclassified and classified computing environments at Livermore, there are need-to-know barriers within the classified computer systems. Access to a classified computing network does not grant users access to all the information in that network. The same need-to-know requirements that apply to verbally communicated information and documents also apply to computer-stored information.

Recent concerns about espionage involving computer-based information and codes spurred a thorough reassessment of computer security at our Laboratory, including threat awareness and training. We support the Secretary of Energy's cyber security initiative and are contributing to his INFOSEC planning.

On April 2, 1999, the Secretary of Energy called for a stand-down of all classified computing at the three DOE national security laboratories. At Livermore, we went even further and shut down all classified computing, all co-located unclassified computing, and all unclassified supercomputing. The stand-down was the first step of a Tri-Lab INFOSEC Action Plan that has been developed and approved by Secretary Richardson. The plan consists of nine action items with specific scheduled milestones. We have met all milestones to date. We will continue working with the DOE Office of Chief Information

Officer (CIO) to fully implement the Tri-Lab INFOSEC Action Plan and further enhance cyber security at the Laboratory.

In addition, on June 21-22, we conducted a two-day-long Security Immersion Program at Livermore to accelerate the security initiatives launched by Secretary Richardson in April. Supervisors were instructed to ensure that all Laboratory employees complete the program, which was directed toward five objectives identified by the Secretary to strengthen security at the laboratories, assessing security issues in individual work areas, and applying what has been learned to each individual's workplace.

We have taken dramatic steps to focus the attention of all Laboratory employees on the threat of foreign intelligence sources as related to cyber security. All employees (including those who do not normally use computers but could have need or access in the future) received special computer security training. We also trained subcontractor employees and consultants. All computing was discontinued until training was complete for all employees on site. Employees who were on travel or leave were trained immediately upon their return. In addition, we have since expanded our on-going computer security training and threat awareness training for all Laboratory personnel using classified computers. This training is unclassified and accessible via a Web site to make it readily available to our employees and easy to update.

Every computer work area and environment at Livermore was evaluated and changes were made as necessary to ensure that LLNL classified and sensitive computing meet the highest standards of information security. In particular:

- We have also taken measures to preclude the transfer of information from classified to unclassified computers in a single work area by the use of removable media.

- We have instituted two-person controls over the authorized transfer of unclassified information from classified computers to unclassified computers.
- Until a more permanent security fix is in place, since April 2, 1999, we have temporarily disabled the file interchange system on the classified supercomputer so that it is impossible to transfer files from the classified supercomputers or the archives to an unclassified computer.
- We also have begun to scan outgoing presumably unclassified e-mail as well as computer files for possible sensitive or classified information. To date, we have scanned over 4 million files in our effort to ensure there is no classified material in unclassified computer files. No issues have arisen.
- We have strong need-to-know controls on our classified network; yet we are investigating ways to provide an even greater level of protection. We are also studying how to apply these same concepts to the unclassified systems to provide better protection to unclassified sensitive information.

In addition, I have also created a Computer Security Policy Board comprised of senior managers to both develop policies and advise me on matters related to unclassified computer security. (Classified computer security policy is defined by DOE Orders.)

On our unclassified computing network, we are improving the way we protect unclassified sensitive information. Some information must be available worldwide, but other information must be protected for privacy, proprietary, or export control reasons. We are implementing additional "firewalls" within our unclassified network to separate fully accessible information from unclassified sensitive information. For several years, Livermore has had an ongoing program to annually scan/audit a sub-set of its unclassified computer systems for security vulnerabilities. We have expanded this policy so that now

all unclassified computer systems must be scanned at least once a year and that appropriate correction/fixes to detect vulnerabilities must be undertaken immediately.

The Laboratory has long had a policy of monitoring users accessing our computer resources via the Internet. We have now expanded our monitoring to cover all dial-in access to Livermore computers. Any Foreign Nationals (FNs) with dial-in capabilities are monitored. Additionally, any FN granted access to unclassified computer resources must first have a programmatic justification of need by the sponsoring Laboratory program and an approved security plan on record for each FN. The Laboratory required that all FNs with access to computer resources had to be recertified by June 30, 1999. No one was "grandfathered" in under our process and those not recertified are being denied access to the computer resources. Certification refers to having a programmatic justification and a security plan in place. Livermore will require that all FNs granted access to Laboratory computer resources must be processed through the Foreign Visits and Assignments Office. This will ensure that any FN with access to Laboratory computer resources will have met the necessary criteria and that their access to computer resources is being monitored.

Finally, our Laboratory is working with personnel at Sandia, Los Alamos, and DOE to develop a "best in practice" plan for cyber security. So far, we have completed a benchmarking of several organizations inside and outside of the government to determine what others are doing to protect information from both outsiders and insiders. This planning activity has an oversight board that is currently being staffed with cyber security professionals from industry along with the CIOs from the three laboratories.

Our approach to cyber security goes beyond addressing vulnerabilities or problems that we identify or that are brought to our attention. We are using this cyber security upgrade as an opportunity to apply our multi-disciplinary approach to science and technology to

become a model for cyber security. Leading-edge cyber security is vital to our programmatic missions and is an area where we can leverage our expertise to enhance national security in the broadest sense.

CLOSING REMARKS

Accomplishing our national security mission requires outstanding science and technology. Simultaneously, we must ensure that the application of that science and technology to national security is protected at all levels. We have long recognized the inherent challenge involved in protecting national security information while fostering the interchange of ideas required for cutting-edge science and technology. Indeed, to a considerable degree, the nation's security rests on the technological advances that arise from the world-class R&D conducted at Livermore and the other national security laboratories.

A multi-faceted security apparatus is in place at our Laboratory, including physical security, operational security, personnel security, information security, communications security, cyber security, counterintelligence, and employee security awareness. We continually make adjustments and upgrades to address new threats and concerns. We take strong positive action on security and counterintelligence issues, whether they are anticipated or identified by us or others, or are brought to our attention in the form of executive or departmental orders or inspections. Proactive and effective security and counterintelligence allows us to meet the challenge of ensuring national security while operating in a global world.

The recent evaluation conducted by OSE noted many improvements to LLNL's security system while identifying areas for further improvement. We have prepared an aggressive

corrective action plan that, technology permitting, will resolve any issues by the end of the year. I have committed the resources and established the priority to ensure that this plan is executed. Corrective actions have already been taken on many issues and, as appropriate, compensatory actions are in place. I am confident that at LLNL, our Special Nuclear Material and sensitive and classified information are secure.

v3.3
7/19/99
dkf